

# Rekordowa kara UODO

## Wnioski dla Twojej firmy

### W TYM WYDANIU:

18 mln zł kary dla ING Banku Śląskiego

1

- Skanowanie dowodów osobistych rodzi ryzyko kar

2

- Konsekwencje dla banku

3

- Wnioski dla Twojej organizacji

3

SZBI - ukryte korzyści

4



Natalia Dzieciuchowicz  
Data Protection Expert

# 18 mln zł kary dla ING Banku Śląskiego

Wnioski dla Twojej organizacji

Decyzją z 23 lipca 2025 Prezes Urzędu Ochrony Danych Osobowych (UODO) nałożył administracyjną karę pieniężną na ING Bank Śląski S.A. Kara wyniosła aż 18,4 mln zł. Jest to najwyższa kara, jaką PUODO nałożył na podmiot z sektora prywatnego.

## Najwyższe kary RODO w Polsce



27 000 000 zł



18 416 400 zł



16 932 657 zł

## Jakie były powody nałożenia kary na bank?

Powodem tak znaczącej sankcji było **nadmierne kopiowanie dokumentów tożsamości klientów i potencjalnych klientów**, co stanowiło naruszenie jednej z podstawowych reguł RODO, czyli **zasady**

**minimalizacji danych**. Pełna treść decyzji dostępna jest [tutaj](#).

Organ stwierdził naruszenie:

- art. 5 ust. 1 lit. a), lit. b) i lit. c)
- art. 6 ust. 1 RODO,

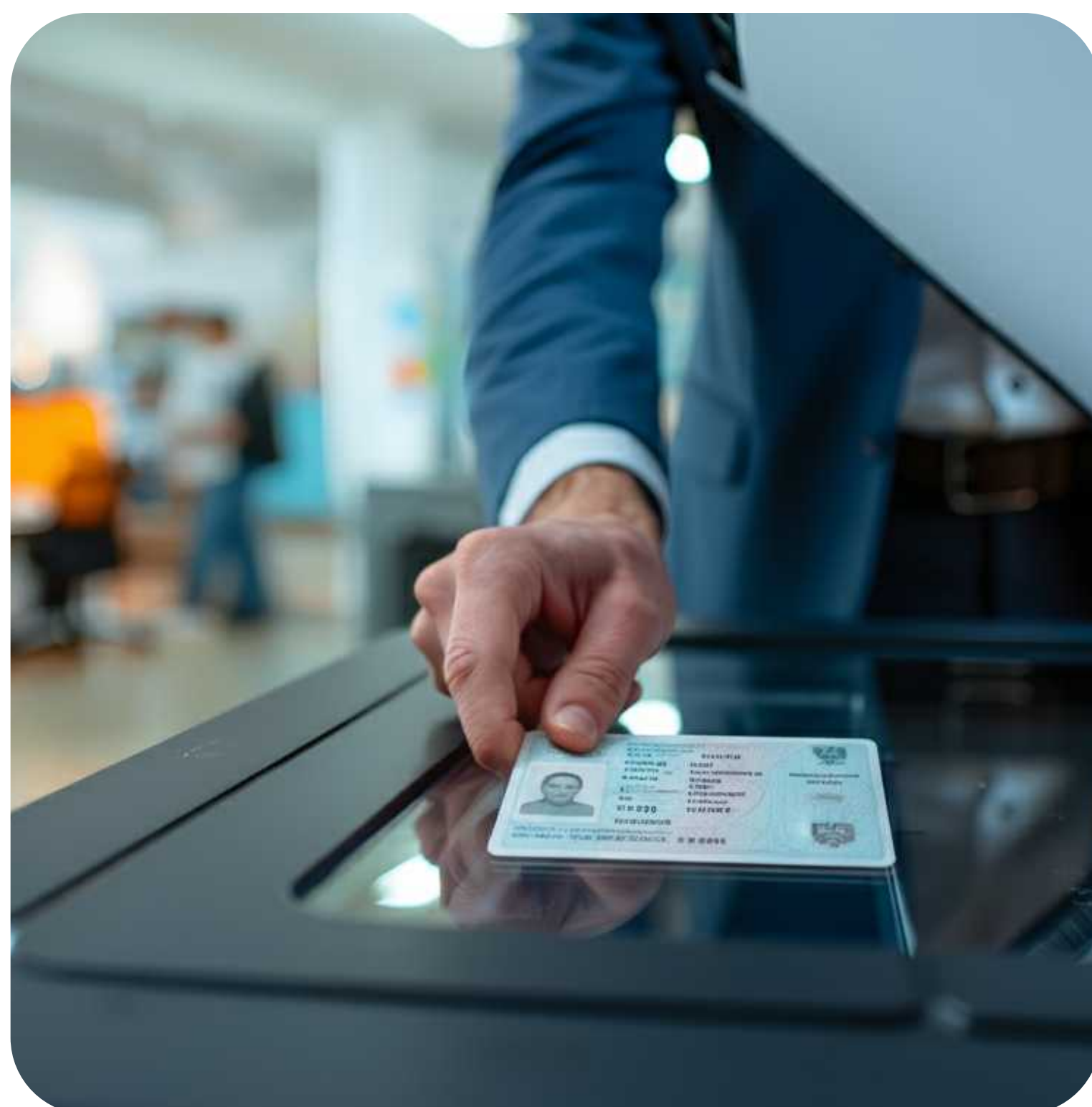
polegające na bezpodstawnym przetwarzaniu danych osobowych obecnych i potencjalnych klientów, pozyskiwanych poprzez skanowanie dokumentów tożsamości w sytuacjach niepowiązanych z obowiązkami banku wynikającymi z ustawy AML (ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu).

**Skanowanie dowodów tożsamości przez instytucje obowiązuje jest legalne w kontekście ustawy AML jedynie wtedy, gdy wiąże się z koniecznym z punktu widzenia tej ustawy zastosowaniem środków bezpieczeństwa finansowego mających na celu przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu.**

Natomiast ING skanował dokumenty także w przypadkach niewiążących się z realizacją obowiązków określonych przepisami ustawy AML (np. przy reklamacji dotyczącej bankomatu).

UODO podkreślił, że kopiowanie dokumentów jest uprawnieniem przysługującym instytucjom obowiązany i nie można uznać, że na podmiotach tych spoczywa obowiązek kopiowania dokumentów tożsamości. Sama procedura identyfikacji klientów jest oczywiście obowiązkowa – wymaga tego prawo. **Problem polegał jednak na tym, że bank kopiował więcej danych, niż było to konieczne i nie udokumentował właściwie, dlaczego taka praktyka była niezbędna.** Bank nie dokonywał indywidualnej oceny ryzyka wiążącego się z danym klientem i podejmowanymi przez niego działaniami.

UODO podkreślił, że bank nie może skanować dowodów osobistych klientów bez stosownej analizy celowości. ING zapowiedziało odwołanie od decyzji, tłumacząc, że pobierało skany dowodów jedynie w sytuacjach niezbędnych do realizacji obowiązków wynikających z ustawy.



## Z jakimi konsekwencjami zmierzył się bank po wydanej decyzji

Podstawowe, dotkliwe konsekwencje to oczywiście kara finansowa. **18,4 mln zł to ogromny koszt nawet dla tak dużej organizacji.** W ocenie Prezesa UODO nałożona na bank kara jest nie tylko skuteczna, ale również proporcjonalna: zarówno do powagi naruszenia jak i do wielkości administratora (mierzoną jego obrotom) a także odstraszająca, a więc spełnia funkcje o których mowa w art. 83 ust. 1 RODO.

Oprócz namacalnych kosztów finansowych bank z dużym prawdopodobieństwem, będzie się również zmagał z kosztami reputacyjnymi. **Sprawa była szeroko opisywana w mediach i niewątpliwie wpłynęła na zaufanie klientów, partnerów biznesowych i samych pracowników (którzy wypełniając obowiązki służbowe de facto naruszali prawo).** Do powyższych dochodzą jeszcze koszty operacyjne związane m.in. z koniecznością zmiany procedur obowiązujących w banku.

## Wnioski dla Twojej organizacji

Warto potraktować tę sprawę jako ostrzeżenie, nawet jeśli Twoja firma działa na mniejszą skalę niż ING.



Mirosław Wróblewski, Prezes UODO

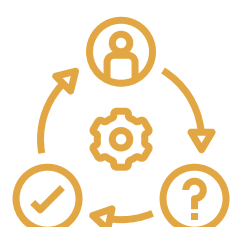
## Wnioski



W procesach przetwarzania danych, które realizujesz w codziennej pracy po pierwsze **zbieraj tylko te dane, które są niezbędne do realizacji celu** – jeśli nie ma wyraźnej podstawy prawnej, nie gromadź dodatkowych informacji.



Po drugie, **dokumentuj swoje działania** – zawsze posiadaj uzasadnienie, dlaczego dane są potrzebne oraz z czego wynika taki a nie inny ich zakres. Dokumentowanie działań zapewnia ponadto spełnienie zasady rozliczalności, której przestrzeganie jest jednym z podstawowych obowiązków wynikających z RODO.



**Aktualizuj procedury** – przepisy się zmieniają, a praktyki, które były akceptowalne kilka lat temu, dziś mogą być ryzykowne.



**Pamiętaj o zachowaniu równowagi** – kluczowe jest realizowanie obowiązków wynikających z przepisów prawa w spójny i komplementarny sposób (w opisywanym przypadku obowiązków wynikających z AML i wymogów RODO).

## Podsumowanie:

Sprawa ING Banku Śląskiego pokazuje, że nawet duże i doświadczone instytucje mogą popełniać błędy, gdy nadmiernie rozszerzają interpretację swoich obowiązków. **Najważniejsze przesłanie dla wszystkich organizacji wydaje się być jednoznaczne: przetwarzać tylko niezbędne do realizacji celu dane, w sposób przemyślany, udokumentowany i uzasadniony. Nie gromadzić ich „na zapas” i bez podstawy prawnej.** Ochrona danych to bowiem nie tylko obowiązek wynikający z prawa, lecz także fundament budowania zaufania klientów i partnerów.



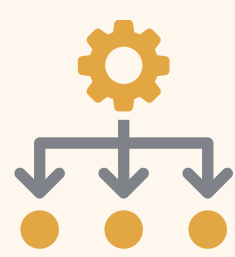


**Dariusz Janiak**  
Information Security & Data Protection Expert

# SZBI - ukryte korzyści

System Zarządzania Bezpieczeństwem Informacji opłaca się z wielu powodów, nie tylko tych związanych ze swoją nazwą.

## SZBI:



### Porządkuje strukturę organizacyjną

— dublujące się procesy są korygowane na etapie projektowania systemu



### Wprowadza klarowny podział ról i obowiązków



### Pozwala na efektywne wykorzystywanie zasobów

— a więc inwestowanie w te zagadnienia, które są faktycznie ważne i istotne dla organizacji

## SZBI pozwala ciąć koszty

System pomaga też uniknąć **nieuzasadnionych wydatków na rozbudowane zabezpieczenia**. Każda organizacja potrzebuje innych rozwiązań z tego zakresu. Inne ryzyka mogą czyhać na instytucje finansowe, a inne na firmy transportowe czy działające w branży IT. Inwestycje mają sens jedynie wówczas, gdy solidnie zinwentaryzujemy zasoby i określimy zagrożenia. Często okazuje się, że proste zmiany organizacyjne mogą dać lepsze rezultaty od złożonych, ale oderwanych od kontekstu organizacji planów.

## ISO 27001 - nowy standard rynkowy

Rynek premiuje firmy, które honorują standardy ISO 27001, zwłaszcza jeśli mogą to udowodnić stosownymi certyfikatami. **Rynek premiuje także te firmy, które stosują się do przepisów NIS2, DORA czy RODO.** SZBI to jasny sygnał, że jest się partnerem godnym zaufania.

## Skutki incydentów mogą być opłakane

Incydentów bezpieczeństwa często nie da odkręcić. Następuje drastyczny spadek zaufania, które ciężko odbudować. Do tego dochodzą bardziej namacalne straty, wynikające z utraty danych, zahamowania działania firmy czy nałożenia kar. Szacuje się, że średni koszt incydentu to [2 miliony dolarów](#), a są przypadki, w których te kwoty są o wiele wyższe.

## Klucz do skutecznego wdrożenia

Aby skutecznie zarządzać bezpieczeństwem, trzeba przyjąć odpowiednie kryteria. Dostępnych jest wiele rozwiązań, a najpopularniejsze z nich to:



**ISO 27001**



**ISO 27002**

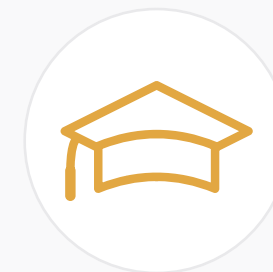
które stanowi rozwinięcie  
wymagań poprzedniej  
normy



**VDA TISAX**

dla branży automotive

**Kluczowe jest to, aby przyjąć te kryteria, a następnie doprowadzić do ich spełnienia.**



## Akademia LexDigital

Powyższy artykuł zawiera treść wykładu z nowego cyklu "Akademia LexDigital", który będzie pojawiać się na naszych kontach na [YouTube](#) i [LinkedIn](#).

W kolejnych odcinkach będziemy szczegółowo wyjaśniać kwestie dotyczące zarządzania dostępem do zasobów organizacji, kryptografii oraz praktycznego podejścia do zarządzania incydentami bezpieczeństwa informacji, uwzględniając też kluczowe ICT. Podamy też przepis na skuteczne szkolenia. Zachęcamy do subskrybowania i udostępniania!





 LexDigital

Pomożemy Ci wdrożyć ISO 27001, nie paraliżując codziennej pracy.

Nasze wybrane realizacje:

 Trafford

 Przelewy24

 merixstudio

Newsletter RODO

Październik 2025 nr 9/2025

# Dziękujemy za przeczytanie naszego newslettera!

Masz pytania?

SKONTAKTUJ SIĘ Z NAMI

 LexDigital

[lexdigital.pl](https://lexdigital.pl)

[LinkedIn](#)